

POWERED BY **Dialog**

User authentication system in personal computer, uses either fingerprint or password for user authentication

Patent Assignee: TOSHIBA KK

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Week	Type
JP 2002222022	A	20020809	JP 200119476	A	20010129	200267	B

Priority Applications (Number Kind Date): JP 200119476 A (20010129)

Patent Details

Patent	Kind	Language	Page	Main IPC	Filing Notes
JP 2002222022	A		13	G06F-001/00	

Abstract:

JP 2002222022 A

NOVELTY A controller prompts the user to input fingerprint data or password during logging-in, based on the working condition of the in-built fingerprint sensor and collates the input data with registered one for authorizing the access of system by the user.

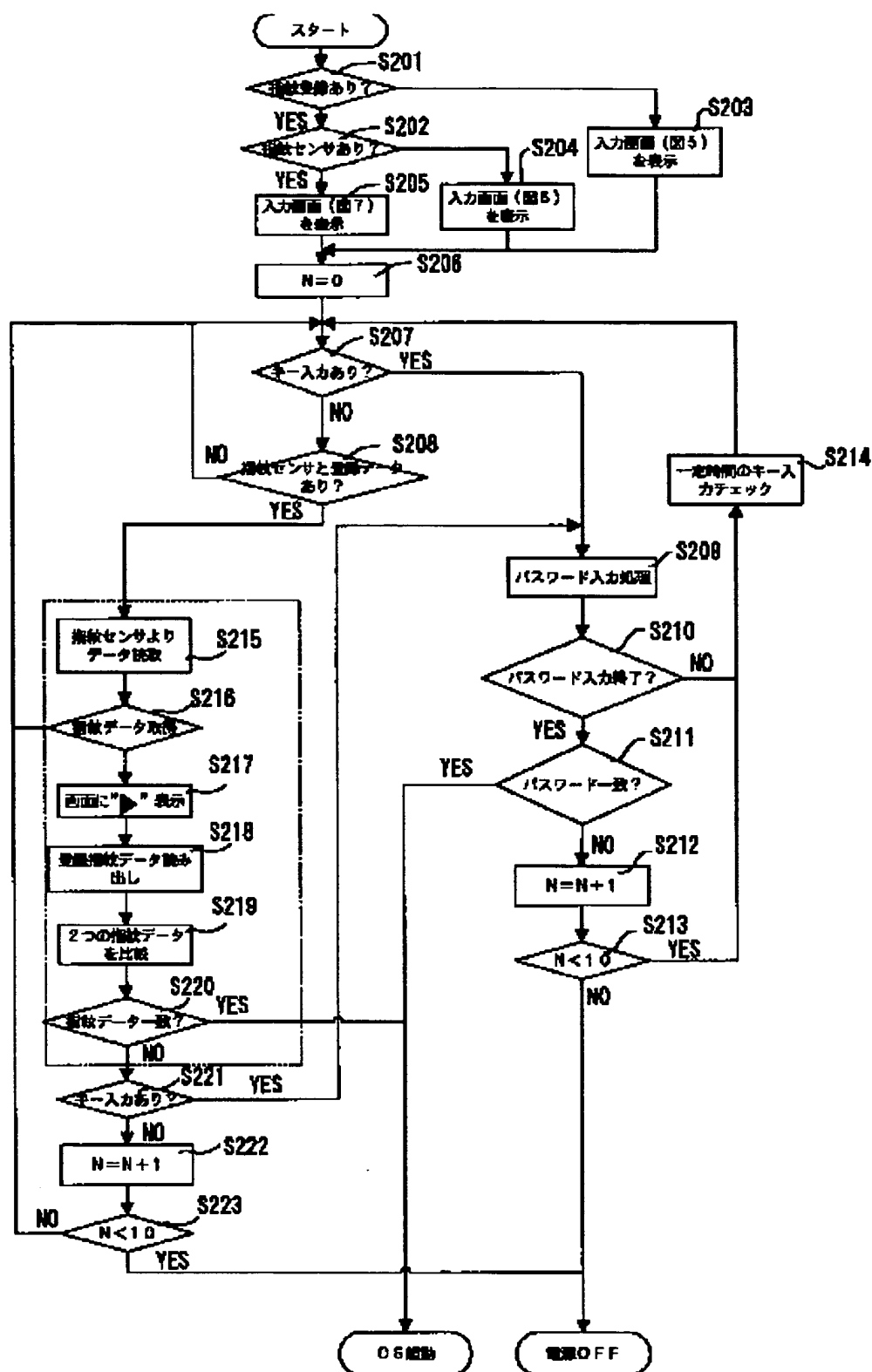
DETAILED DESCRIPTION An INDEPENDENT CLAIM is included for the user authentication method.

USE For user authentication in personal computer like laptop.

ADVANTAGE The authorization is more easier as it uses either fingerprint data or password for authorization.

DESCRIPTION OF DRAWING(S) The figure shows a flowchart explaining the fingerprint authentication. (Drawing includes non-English language text).

pp; 13 DwgNo 3/15



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-222022
(P2002-222022A)

(43)公開日 平成14年8月9日(2002.8.9)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 E 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 F

審査請求 未請求 請求項の数13 O L (全 13 頁)

(21)出願番号 特願2001-19476(P2001-19476)

(22)出願日 平成13年1月29日(2001.1.29)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 田村 聡

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74)代理人 100083161

弁理士 外川 英明

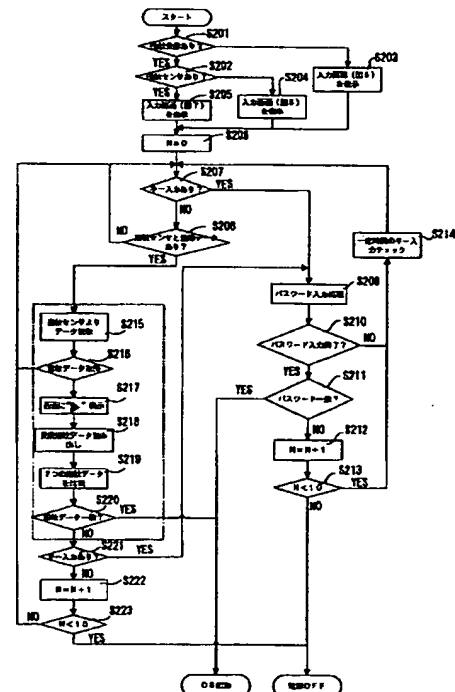
Fターム(参考) 5B085 AE03 AE26

(54)【発明の名称】 電子機器システム及び電子機器システムの起動方法

(57)【要約】

【課題】 OS起動前のユーザ認証方法として、パスワードか生体データのどちらか一方が登録しておいたデータと一致すればOSが起動する電子機器の起動方法を提供することを目的とする。

【解決手段】 システムの電源がONされると、制御部3は、ユーザ識別データ保存部6に指紋データが登録されているか否か、また、指紋センサ2が使用可能であるか否かを判断し、予め指紋が登録されていない、又は指紋センサ2が使用可能状態に無い場合は、表示部6にパスワードの入力を促す画面を表示する。予め指紋データ登録済みで且つ指紋センサ2が使用可能状態であれば、指紋データ若しくはパスワードのどちらかの入力を促す画面を表示部6に表示する。入力されたデータと登録済みのデータとを照合し、照合結果に応じてシステムの起動可否を決定し、OS起動/シャットダウンの処理を行う。



【特許請求の範囲】

【請求項1】 使用者の本人確認を行う電子機器システムであって、前記使用者の生体データを入力する手段と、パスワードを入力する文字入力手段と、前記使用者の生体データ及びパスワードを予め記憶する記憶手段と、前記電子機器システムへの電源投入時に、生体データ又はパスワードを入力する旨の指示を提示する指示手段と、前記生体データ入力手段から生体データを入力された場合は、前記記憶手段に記憶されている生体データとの照合を行ない、前記文字入力手段からパスワードの入力があつた場合は、前記記憶手段に予め記憶されているパスワードとの照合を行なう照合手段と、前記照合手段の照合結果に応じて、前記電子機器システムの使用可否を制御する制御手段とを具備することを特徴とする電子機器システム。

【請求項2】 前記生体データは、使用者の指紋データであることを特徴とする請求項1に記載の電子機器システム。

【請求項3】 前記生体データ入力手段はPCカードであり、前記電子機器システムに着脱可能に接続することを特徴とする請求項1に記載の電子機器システム。

【請求項4】 前記制御手段はさらに、前記記憶手段に予め生体データが記憶されているか否かを判断し、前記記憶手段に予め生体データが記憶されていないと判断した場合、前記指示手段へパスワードの入力のみを促すことを指示し、前記指示手段は、パスワードの入力のみを促すことを特徴とする請求項1に記載の電子機器システム。

【請求項5】 前記記憶手段に記憶されている前記パスワードを削除する場合、前記記憶手段に記憶している生体データも削除することを特徴とする請求項1に記載の電子機器システム。

【請求項6】 電子機器本体と、前記電子機器本体に着脱可能に接続する生体データ入力部とからなり、使用者の本人確認を行う電子機器システムであって、前記生体データ入力部は、前記使用者の生体データを入力する手段と、前記生体データを用いて、使用者の確認を実行するプログラムを記憶する第1の記憶手段とを具備し、前記電子機器本体は、パスワードを入力する文字入力手段と、前記使用者の生体データ及びパスワードを予め記憶している第2の記憶手段と、使用者に、生体データまたはパスワードの入力の操作を促す指示手段とを具備し、前記電子機器本体はさらに、前記第1の記憶手段から前記プログラムを読み込み、前記指示手段により生体データまたはパスワードの入力を促し、前記生体データ入力部から生体データの入力が行なわれた場合は、前記第2の記憶手段に記憶されている生体データとの照合を行ない、前記文字入力手段からパスワードの入力があつた場合は、前記パスワードとの照合を行なう照合手段と、前記照合手段の照合結果に応じて、前記電子機器本体の使用可否を制御する制御手段とを具備することを特徴とする

る電子機器システム。

【請求項7】 前記生体データは、使用者の指紋データであることを特徴とする請求項6に記載の電子機器システム。

【請求項8】 前記生体データ入力部は、PCカードであり、前記電子機器本体が具備するPCカードスロットルに着脱可能に接続することを特徴とする請求項6に記載の電子機器システム。

【請求項9】 前記第2の記憶手段に記憶している前記パスワードを削除する場合、前記第2の記憶手段に記憶している生体データも削除することを特徴とする請求項6に記載の電子機器システム。

【請求項10】 前記生体データ入力部が前記電子機器本体に接続していない場合、若しくは前記第2の記憶手段に予め生体データが記憶されていない場合、前記指示手段は、パスワードの入力指示のみを促す指示を出すことを特徴とする請求項6に記載の電子機器システム。

【請求項11】 生体データを入力する手段と、パスワードを入力する手段とを具備する電子機器システムの起動方法であって、使用者に、生体データまたはパスワードの入力を促し、前記生体データ入力手段から生体データを入力された場合は、前記電子機器システムが具備する第1の記憶手段に登録している生体データとの照合を行ない、前記文字入力手段からパスワードの入力があつた場合は、前記第1の記憶手段に記憶されているパスワードとの照合を行ない、照合結果に応じて、前記電子機器システムの使用可否を制御することを特徴とする電子機器システムの起動方法。

【請求項12】 前記生体データは指紋データを用いることを特徴とする請求項11に記載の電子機器システムの起動方法。

【請求項13】 生体データを入力する生体データ入力手段と、パスワードを入力する文字入力手段とを具備する電子機器システムの起動方法であって、前記電子機器システムの電源が投入された際に、予め使用者の生体データが登録されているか否かを判断し、前記生体データ入力手段が使用可能であるか否かを判断し、予め生体データの登録が成されており且つ前記生体データ入力手段が使用可能状態である場合は、生体データ、若しくはパスワードの入力を促し、前記生体データ入力手段から生体データを入力された場合は、予め登録されている生体データとの照合を行ない、前記文字入力手段からパスワードの入力があつた場合は、予め登録されているパスワードとの照合を行ない、照合結果に応じて、電子機器システムの使用可否を制御し、前記生体データが登録されていない場合、若しくは前記生体データ入力手段が使用不可能状態である場合は、パスワードの入力を促し、前記文字入力手段から入力されるパスワードと、予め登録されているパスワードとの照合を行い、照合結果に応じて、電子機器システムの使用可否を制御することを特徴とする

電子機器システムの起動方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、生体データを用いる電子機器システムおよび電子機器システムの起動方法に関する。

【0002】

【従来の技術】従来、パーソナルコンピュータ（以後、パソコンと称す）等の電子機器を起動する際に、特定ユーザを認証する方法として、文字・数字の組合せから成るパスワードを照合して、ユーザを認証する方法（以後、パスワード認証方法と称す）が用いられている。

【0003】また、近年、パスワード認証方法以外にも、指紋に代表される生体データを照合してユーザを認証する方法（以後、指紋認証方法と称す）も急速に普及して来ている。

【0004】特に、指紋認証方法は、1. パスワード方法に比べてキーボードを使った入力を必要としない、2. パスワードのように覚えておく必要がない、3. 指紋情報は他人と異なるなど、簡便さ及びセキュリティ面で有効的な方法である。

【0005】このような指紋認証による電子機器のセキュリティとしては、特開2000-122975公報では、指紋を含む複数のバイオメトリクスデータをユーザ確認手段として用い、ログオン許可などを実現するバイオメトリクスによるユーザ確認システム及び記憶媒体が開示されている。

【0006】また、特登 2967764号公報では、非接触ICカードにより指紋認証を行った結果をコンピュータに送信しログインをしようとした、非接触ICカードおよびそれを用いたログイン方法といった技術が開示されている。

【0007】

【発明が解決しようとする課題】しかし、上記従来技術では、特開2000-122975公報では、確認手段の一つに、生体データを用いるが、使用者側で、ログイン時の照合方式を自由に選択することが可能となっているが、選択した認証方法全てについて、照合をする必要があり、全ての照合について、許可になった場合のみ電子機器のログオン許可となるため、その選択した照合方式が一つでも、マッチしなかった場合にログオンはできない。また、その照合に要する生体データが複数あるため、どの生体データを登録しているのか等データ管理が困難である。

【0008】また、特登 2967764号公報記載の非接触カードを用いる場合では、必ず、カードとシステムとが同じ無線方式に応じたものでことが必要となる。また、カード側に、指紋登録データ及び、パスワードとを記憶しているので、カードを紛失した場合などに、システムにログインすることができなくなるといった問題

がある。

【0009】さらに、ログイン方法が、生体データのみによるものである場合は、例えば指紋のみの認証では指紋に傷がついたときなど、指紋の情報に変化が起こった場合に、ユーザ本人であるのに認証で拒否されてしまい、その後システムへのログインを拒否されることが考えられる。

【0010】そこで、本発明では電子機器システム起動時のユーザ認証方法として、セキュリティ面で有用で且つ、指紋情報に変化が起こった場合でも柔軟に対応可能な電子機器システムおよび電子機器システムの起動方法を提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成する為に、請求項1にかかる発明では、使用者の本人確認を行う電子機器システムであって、使用者の生体データを入力する手段と、パスワードを入力する文字入力手段と、使用者の生体データ及びパスワードを予め記憶する記憶手段と、電子機器システムへの電源投入時に、生体データ又はパスワードを入力する旨の指示を提示する指示手段と、生体データ入力手段から生体データを入力された場合は、記憶手段に記憶されている生体データとの照合を行ない、文字入力手段からパスワードの入力があつた場合は、記憶手段に予め記憶されているパスワードとの照合を行なう照合手段と、照合手段の照合結果に応じて、電子機器システムの使用可否を制御する制御手段とを具備することを特徴とする。

【0012】このような構成により、電子機器起動時の使用者認証において、生体データもしくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データに変化が起き、生体データによる使用者認証ができなくなった場合でも、パスワードによる使用者認証が可能であり、使用者認証が柔軟に対応可能である電子機器システムを提供することが可能となる。

【0013】また、請求項6にかかる発明では、電子機器本体と、電子機器本体に着脱可能に接続する生体データ入力部とからなり、使用者の本人確認を行う電子機器システムであって、生体データ入力部は、使用者の生体データを入力する手段と、生体データを用いて、使用者の確認を実行するプログラムを記憶する第1の記憶手段とを具備し、電子機器本体は、パスワードを入力する文字入力手段と、使用者の生体データ及びパスワードを予め記憶している第2の記憶手段と、使用者に、生体データまたはパスワードの入力の操作を促す指示手段とを具備し、電子機器本体はさらに、第1の記憶手段からプログラムを読み込み、指示手段により生体データまたはパスワードの入力を促し、生体データ入力部から生体データの入力が行なわれた場合は、第2の記憶手段に記憶されている生体データとの照合を行ない、文字入力手段からパスワードの入力があつた場合は、パスワードとの照

合を行なう照合手段と、照合手段の照合結果に応じて、電子機器本体の使用可否を制御する制御手段とを具備することを特徴とする。

【0014】このような構成により、電子機器起動時の使用者認証において、生体データによる認証が可能か否か判断し、生体データ認証が可能な場合は、生体データ若しくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データ認証ができない場合は、パスワードの認証を使用者に促し、状況に応じて、認証処理を柔軟に対応可能とする電子機器システムを提供することが可能となる。

【0015】また、請求項11にかかる発明では、生体データを入力する手段と、パスワードを入力する手段とを具備する電子機器システムの起動方法であって、使用者に、生体データまたはパスワードの入力を促し、生体データ入力手段から生体データを入力された場合は、電子機器システムが具備する第1の記憶手段に登録している生体データとの照合を行ない、文字入力手段からパスワードの入力があつた場合は、第1の記憶手段に記憶されているパスワードとの照合を行ない、照合結果に応じて、電子機器システムの使用可否を制御することを特徴とする。

【0016】このような構成により、電子機器起動時の使用者認証において、生体データもしくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データに変化が起き、生体データによる使用者認証ができなくなった場合でも、パスワードによる使用者認証が可能であり、使用者認証が柔軟に対応可能である電子機器システムの起動方法を提供することが可能である。

【0017】また、請求項13にかかる発明では、生体データを入力する生体データ入力手段と、パスワードを入力する文字入力手段とを具備する電子機器システムの起動方法であって、電子機器システムの電源が投入された際に、予め使用者の生体データが登録されているか否か判断し、生体データ入力手段が使用可能であるか否か判断し、予め生体データの登録が成されており且つ生体データ入力手段が使用可能状態である場合は、生体データ、若しくはパスワードの入力を促し、生体データ入力手段から生体データを入力された場合は、予め登録されている生体データとの照合を行ない、文字入力手段からパスワードの入力があつた場合は、予め登録されているパスワードとの照合を行ない、照合結果に応じて、電子機器システムの使用可否を制御し、生体データが登録されていない場合、若しくは生体データ入力手段が使用不可能状態である場合は、パスワードの入力を促し、文字入力手段から入力されるパスワードと、予め登録されているパスワードとの照合を行い、照合結果に応じて、電子機器システムの使用可否を制御することを特徴とする。

【0018】このような構成により、電子機器起動時の

使用者認証において、生体データによる認証が可能か否か判断し、生体データ認証が可能な場合は、生体データ若しくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データ認証ができない場合は、パスワードの認証を使用者に促し、状況に応じて、認証処理を柔軟に対応可能とする電子機器システムの起動方法を提供することが可能である。

【0019】

【発明の実施の形態】以下本発明に係る実施の形態を、図面を参照して説明する。

【0020】本実施形態では、生体データとして、指紋データを用いる例について説明する。

【0021】図1に、本実施形態に係る、電子機器システムのハードウェア構成図を示す。

【0022】ユーザインターフェースとして、キーボード1と指紋センサ2を具備し、これらは、システム全体の制御および、ログイン認証処理の制御を司る制御部3に接続している。

【0023】この制御部3には、ログイン認証処理の認証プログラムを保存する認証プログラム保存部4と、ユーザが登録したパスワードおよび指紋データを保存するユーザ識別データ保存部5とが接続している。

【0024】また、ユーザに対し、各種情報や操作を促すための情報を提示するための表示部6も、制御部3と接続している。

【0025】キーボード1は、本システムのユーザインターフェースの1つであり、通常は、システムの操作を行なうが、文字・数字の組合せから成るパスワードを入力する際にも用いる。

【0026】指紋センサ2は、指紋データを入力する際のインターフェースであり、表示部6に表示される指示に従い、指紋センサ2に指を接触させることにより、ユーザの指紋を読み込むものである。この指紋センサ2は、このシステムに内蔵されるものも考えられるが、その他に、PCカードのものや、USBにより接続するものなどが考えられる。

【0027】制御部3は、システム全体の制御を司り、認証プログラム保存部4から、指紋認証プログラムを読み出し、認証プログラムを実行、制御するものである。

【0028】認証プログラム保存部4は、後述する指紋認証プログラムを記憶しており、制御部3により読み出される。

【0029】ユーザ識別データ保存部5は、ユーザが登録した文字・数字から成るパスワード及びユーザの指紋データを記憶保存するものであり、ユーザ毎にパスワードと指紋データとを記憶している。

【0030】表示部6は、ユーザに対して視覚的に情報を提示するものであり、CRTやLCDなどの表示装置が用いられる。

【0031】図2に、電子機器システムの例の斜視図を

示す。

【0032】本発明に係る電子機器システムの例として、図2のようなパソコン13が挙げられる。

【0033】パソコン13は、本体ケース12と表示部ケース13と表示部6とキーボード1とを有する。本体ケース12はその上部にキーボード1を配設している。本体ケース12と表示部ケース13とは、ヒンジ部14により回動可能に接続している。表示部ケース13は、表示部6の表示領域が可視状態となるよう表示部6の周辺部を保持している。本体ケース12側面にはPCカードを着脱可能に接続するPCカードスロット15を有し、このPCカードスロット15に、PCカードの形で提供される指紋センサ2が挿入している。

【0034】次に、まずユーザ認証の核となる指紋認証の処理について図3を用いて説明する。図3は、指紋認証プログラムのフローチャートである。

【0035】まず、制御部3が認証プログラム保存部4から、指紋認証プログラムを読み出し（ステップS101）、以後説明する認証プログラムを実行する。

【0036】指紋認証プログラムでは、まず指紋センサ2からユーザの指紋データを読取る（ステップS102）。ここで、指紋センサ2により指紋データが読取れなければ（ステップS102のNO）、エラー処理1を行なう（ステップS103）。

【0037】エラー処理1は、表示部6に、指紋データが読み取れない旨のメッセージの表示を行ったり、図示しないスピーカから警告音を発生させるなど、ユーザに読取エラーであることを通知する。

【0038】指紋センサ2により指紋データが読取れた場合（ステップS102のYES）、次のステップで既に登録されている指紋データ（以後、既登録データと称す）との比較を行なう。

【0039】指紋データが読み取れた際に、制御部3がユーザ識別データ保存部5から、既登録データを読み出す（ステップS104）。指紋センサ2により読みとった指紋データ（以後、認証対象データ）と、既登録データとを比較し（ステップS105）、2つのデータが一致していた場合には（ステップS105のYES）、ユーザ認証成功となり指紋認証処理を終了する。

【0040】ここで、ユーザ識別データ保存部6に複数の指紋データが登録されている場合には、これら複数の既登録データと認証対象データとの比較を繰り返す。

【0041】既登録データと認証対象データとが一致しない場合（ステップS106のNO）、エラー処理2を行なう（ステップS107）。エラー処理2では、表示部6に指紋センサ2により読みとった指紋データが、既登録データと一致しない旨のメッセージを表示させる。また、さらに他の指を指紋センサにより読み取るように促すメッセージを表示しても良い。

【0042】上記のように、ユーザの指紋認証処理が行

なわれる

【0043】続いて、上述した指紋認証プログラムを利用して、パスワードまたは指紋によるユーザ認証処理を行なうフローチャートを図4に示す。

【0044】まずシステムの電源がONされると、制御部3は、ユーザ識別データ保存部6に指紋データが登録されているか否かをチェックする（ステップS201）。

【0045】なんらかの指紋データが登録されていると（ステップS201のYES）、次に指紋センサ2の有無を確認する（ステップS202）。これは、指紋センサ2がPCカードの形状をしたものや、USBにより接続するものである場合や、別途電源供給を受けている場合などが考えられるためであり、指紋センサ2が使用可能であるか否かを判断する。

【0046】上記ステップS201とステップS202の判定により表示部6に表示する入力画面を3種類に分ける。

【0047】指紋が登録されていない場合（ステップS201のNO）は、図5に示す入力画面を表示部6に表示し（ステップS203）、指紋データは登録されているが（ステップS201のYES）、指紋センサ2が無い（電源OFF、非接続等）場合（ステップS202のNO）は、図6に示す入力画面を表示部6に表示する（ステップS204）。指紋データが登録されており（ステップS201のYES）、且つ指紋センサ2がある（電源ON、接続済み等）場合（ステップS202のYES）は図7に示す入力画面を表示部6に表示する（ステップS205）。

【0048】図5乃至図7に示す入力画面は、ユーザに対して、ユーザがどのような認証処理を行えば良いのかを明確にするためである。

【0049】夫々、入力画面表示後、ユーザ認証エラーの際に、リトライの機会を与える為のエラーカウント変数“N”を0にセットする（ステップS206）。

【0050】まず、指紋センサ若しくは登録された指紋データ（既登録データ）が無い場合について説明する。

【0051】指紋センサ2及び既登録データが無い場合は、指紋認証を行うことができ無いため、パスワードによるログイン処理のみを行なう。よってステップS207のキー入力の判定を行ないキー入力が無い場合（ステップS207のNO）は、指紋センサ2若しくは登録指紋データも無いので（ステップS208のNO）、再びステップS207に戻り、キー入力が行なわれるまで、このループを繰り返す。

【0052】キー入力があると（ステップS207のYES）、パスワードによる認証処理を開始する。

【0053】パスワード認証処理（ステップS209）では、キーボード1から入力された数字・文字を保存し、パスワード入力終了する（リターンキーが押され

る) までに入力された文字列をユーザから入力されたパスワードとして判断する。

【0054】パスワード入力終了の判定(ステップS210)でパスワード入力が終了された場合(ステップS210のYES)、入力されたパスワードとユーザ識別データ保存部5に保存されているパスワード(予めユーザが登録しておいたパスワード)との比較をおこなう(ステップS211)。

【0055】パスワード入力が終了していない場合は(ステップS210のNO)、次のキー入力待を為しに一定時間のキー入力チェックを行なう(ステップS214)。キー入力があれば(ステップS207のYES)、再びキーボード1から入力された数字・文字を保存し、パスワード入力終了か否かのチェックを行なう(ステップS210)。

【0056】パスワードが一致した場合には、パスワードが一致したことを表示部6に表示し、OS起動の処理を行なう。パスワードが一致し、認証に成功したときの画面表示例を図8に示す。

【0057】パスワードが一致しなかった場合(ステップS211のNO)は、エラーカウンタ変数“N”を加算する(ステップS212)。次に、所定のエラー許可回数と“N”との値を比較する(ステップS213)。本例では、エラー許可回数を10とする。エラー許可回数を越えていない場合(ステップS213のYES)、一定時間のキー入力待ち(ステップS214)状態から、ステップS207のキー入力処理に戻り、上述したパスワード入力処理を改めて開始する。この際、前回入力されたパスワードをクリアする。

【0058】エラー許可回数を越えていた場合(ステップS211のYES)は電源をOFFする。

【0059】エラー許可回数は、ユーザに入力ミスの猶予を与えるための数値である。ユーザの入力ミスをカウントし、予め決められたエラー許可回数(本例では10回)を越えるまでは、再び認証のための入力処理をおこなうが、エラー許可回数を越えた場合には、OSを使うことのできるユーザではないと判断する。本件ではこの場合の処理として電源OFFをおこなう。

【0060】次に、指紋が登録されていて、且つ指紋センサ2を具備する場合のパスワード認証処理と指紋認証処理について説明する。

【0061】まず、キー入力があるか否かの判断を行い(ステップS207)、キー入力があれば(ステップS207のYES)、前述したパスワード認証処理を行なう。

【0062】キー入力がない場合(ステップS207のNO)は、次に、指紋センサ2と登録指紋データがあるか否かを判断する(ステップS208)。

【0063】ここでは、指紋センサ2も登録指紋データもある場合を想定しているので(ステップS208のY

ES)、指紋認証処理へ進む。図9に指紋認証の画面表示初期状態の図を示す。

【0064】指紋認証処理(点線で囲まれた部分、ステップS215乃至ステップS220)は、途中、画面表示を行う処理(ステップS217)を除いて図3で説明したものと同一である。

【0065】指紋認証処理が開始されると、制御部3は、認証プログラム保存部4から指紋認証プログラムを読取る。

【0066】まず、指紋センサ2から指紋データを読み取る(ステップS215)。指紋データの読取りに成功すると(ステップS216のYES)、図10に示す画面表示例のように指紋データが読み取れたことを表示部6を介して通知する。指紋データの読取りができなければ(ステップS216のNO)、指紋認証処理を終了し、ステップS207へ戻る。

【0067】指紋データが読み取れた場合(ステップS216のYES)、次に読みとった指紋データと、ユーザ識別データ保存部5に記憶している既登録データとの比較を行なう(ステップS219)。指紋データが一致すれば(ステップS220のYES)、指紋データが一致したことを表示部6に表示し、OS起動の処理をおこなう。認証に成功した場合の画面表示例は図8に示したものと同一である。指紋データが一致しない場合には(ステップS220のNO)、キー入力があるか否かの判定を行ない(ステップS221)、キー入力があれば(ステップS221のYES)パスワード認証処理へ移行する。指紋認証に失敗した場合の画面表示例を図11に示す。

【0068】キー入力がない場合は(ステップS221のNO)、エラーカウンタ変数“N”を加算する(ステップS222)。次に、所定のエラー許可回数と“N”との値を比較する(ステップS223)。

【0069】“N”がエラー許可回数以内である場合は、再びステップS207へ戻り、キー入力判定を行なう。

【0070】上記した一連の処理をエラー許可回数(本例では10回)だけ繰り返す。10回連続して指紋認証処理を行なった場合の画面表示例を図12に示す。

【0071】これは10回連続で指紋データを読取ることはできたが、既登録指紋データとは一致しなかったことを示している。また、本件ではエラー許可回数を10回としているが、これは何回でもよく、ユーザにより設定することも可能である。

【0072】10回の指紋認証処理を行ってもユーザ認証ができない場合は(ステップS223のYES)、OSを使うことのできるユーザではないと判断する。本件ではこの場合の処理として電源OFFをおこなう。

【0073】本例ではパスワードと指紋認証とのエラー許可回数を同じ変数“N”同一にカウントしているが、

別々に変数を設けて、夫々エラー許可回数を設定することも可能である。

【0074】上記のように、本発明では、パスワード若しくは指紋データによるユーザ認証処理を行うことが可能であり、ユーザに対して、2通りの認証手段を提示し、どちらかの認証に成功すれば、システムの起動を行なうものである。このことによって、パスワードを忘れてしまった場合は指紋認証によるログインが可能であり、指紋が傷付いてしまった場合などには、パスワードによるログインが可能であるため、様々なアクシデントに柔軟に対応可能な電子機器システム及びその起動方法を提供することが可能となる。

【0075】続いて、サスペンド、休止状態からの復帰の際の認証処理について図13を用いて説明する。図13はサスペンド／休止状態から、PCを使用状態へ復帰する際のフローチャートである。

【0076】図4を用いて説明した処理は、サスペンド、休止状態からの復帰時にも利用可能である。

【0077】まず、サスペンド、若しくは休止状態から、復帰する時に、図4を用いて説明した認証処理が行われる(ステップS301)。

【0078】パスワード若しくは指紋認証によりユーザが認証された場合は(ステップS302のYES)、OSへ復帰する(ステップS303)。

【0079】のような処理を行う。この場合、認証されないときは電源OFFするのではなく、それぞれサスペンド、休止状態に戻す。

【0080】次に、指紋データをユーザ識別データ保存部6へ登録する場合について説明する。

【0081】指紋の登録と削除についてはOS上のユーティリティソフトを用いて行う。図14にユーティリティソフトの画面例を示す。

【0082】図14の指紋ユーティリティ画面11は、パスワードを入力する欄12と、指紋登録及び、指紋データの更新を行うためのボタン13と、指紋データを削除する際のボタン14と、この画面を終了するボタン15が表示される。

【0083】パスワード欄12は、ユーザの登録パスワードを入力するボックスであり、ここで、ユーザのパスワードを入力し、ユーザ確認を行なうと、指紋データの登録／更新および削除を行なうことが可能となる。本指紋登録ユーティリティは、パスワードが登録されていない場合は、指紋登録を行なうことができないようになっている。なお、本例では、このパスワードは、電子機器システム起動時のパスワードと同じものであるが、別に登録するものとしても良い。

【0084】指紋データ登録／更新ボタン13は、ユーザ認証が完了した場合に、そのユーザの指紋データを登録することが可能となる。

【0085】指紋削除ボタン14は、登録済みの指紋デ

ータを削除する場合に用いる。

【0086】キャンセルボタン15は、この指紋ユーティリティ画面11を終了する際に用いるものである。

【0087】次に、指紋データを登録する際の処理について、図15に指紋データ登録のフローチャートを示す。

【0088】まず、指紋データ登録を行なうために指紋ユーティリティソフトを起動する。この際に、ユーザのパスワードがユーザ識別データ保存部5に登録されているか否かのチェックを行い(ステップS401)、パスワードが登録されていない場合は(ステップS401のNO)、ダイアログ等でエラーメッセージの表示を行ないユーティリティを起動しない(ステップS402)。これは、本発明では指紋を登録するためにはそれに対応するユーザのパスワードが必要であるためである。

【0089】パスワードがユーザ識別データ保存部5に登録されていれば(ステップS401のYES)、図14に示すユーティリティ画面11を表示する

【0090】ここで、ユーティリティにパスワードを入力して、指紋登録／更新ボタン13を押すと、パスワードの認証が行われる。ここで、パスワードが間違っていることを表示部6を介してユーザに通知する。パスワードが正しく、認証が成功した場合は、指紋登録処理を開始する。

【0091】指紋登録処理では、指紋センサ2から指紋データの読み取りを行い(ステップS406)、指紋データを読取れば(ステップS407のYES)、そのデータをユーザ識別データ保存部5へと保存する(ステップS408)。指紋データが読取れなかった場合(ステップS407のNO)には、再び指紋データの取得を行うか、登録を終了するかを選択することが可能である(ステップS409)。ここで、再び指紋データの登録を選択すると(ステップS409のYES)、ステップS406に戻り、指紋センサ2から指紋データの読取を行なう。指紋データの登録を終了する場合(ステップS409のNO)は、指紋ユーティリティを終了する。

【0092】また、ステップS408において、指紋データの登録を行なうと、他の指紋データの登録も行なうことが可能である。複数の指紋登録が可能である。

【0093】次に、登録されている指紋データを削除する場合について説明する。

【0094】指紋データの削除は、図14に示した指紋ユーティリティを使って行う。方法は指紋ユーティリティを起動しパスワードを入力後、指紋削除ボタン14を押す。

【0095】パスワードが一致すれば、登録している指紋データを削除することができる。一人で複数登録している場合は、登録されている指紋データがリストとして、表示部6に表示され、削除したい指紋データを選択することができる。

【0096】また、本件ではパスワードの削除を行なうと自動的にそれに対応した指紋も削除される。1人のユーザが複数の指を登録していた場合でも、そのユーザのすべての指紋データが削除される。このように、パスワードと関連付けて指紋データの登録／削除を行なうことで、指紋データのみ依存しないシステムとしている。これは、指紋データのための認証では、指紋が傷ついた時などにシステムの起動ができなくなるためであり、本発明では、指紋認証はあくまでもパスワード認証の代替として機能するものである。

【0097】上述したように、本発明によれば、指紋データ若しくはパスワードのどちらかによって、パソコンへのログイン認証を行なうことが可能となる。

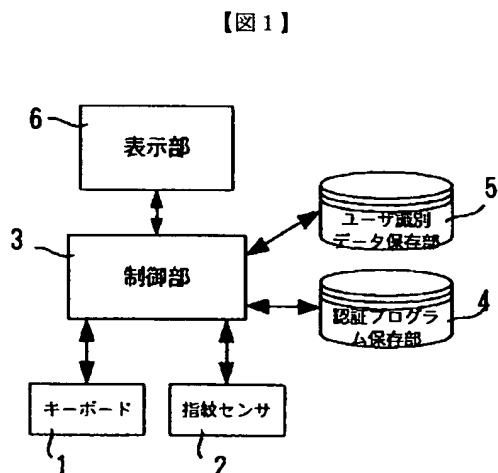
【0098】また、本実施形態では、生体データとして指紋データを用いた例を示したが、その他の生体データ認証として音声認証、顔認証、ハンドライティング署名認証等が考えられる。これらの場合、指紋センサ2の替りに、マイク、カメラ、ペン入力インターフェースが必要となるが、上述した実施例と同様の方法をOS起動前に行なうことによりパスワードまたは生体データ（音声認証、顔認証、ハンドライティング署名など）のどちらか一方によるユーザ認証により、OSを起動することができる。

【0099】

【発明の効果】以上詳述した発明によれば、OS起動前のユーザ認証方法として、パスワードか生体データのどちらか一方が登録しておいたデータと一致すればOSが起動する電子機器の起動方法を提供することが可能である。

【図面の簡単な説明】

【図1】電子機器システムのハードウェア構成図。



【図1】

【図2】電子機器システムの斜視図。

【図3】指紋認証プログラムのフローチャート。

【図4】ユーザ認証処理のフローチャート。

【図5】登録した指紋データが無い場合の表示画面例の図。

【図6】登録した指紋データはあるが、指紋センサが無い場合の表示画面例の図。

【図7】登録した指紋データと指紋センサとがある場合の表示画面例の図。

【図8】認証に成功した場合の表示画面例の図。

【図9】指紋認証初期表示画面例の図。

【図10】指紋データが読み取れた場合の表示画面例の図。

【図11】認証に失敗した場合の表示画面例の図。

【図12】指紋認証処理を行なった場合の表示画面例の図。

【図13】サスペンド、休止状態からの復帰フローチャート。

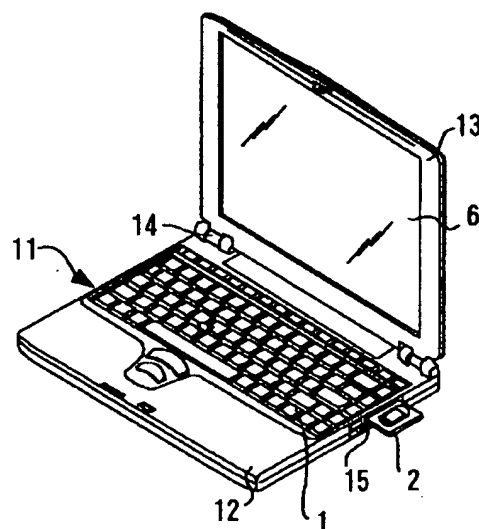
【図14】指紋ユーティリティソフトの画面例の図。

【図15】指紋データの登録フローチャート。

【符号の説明】

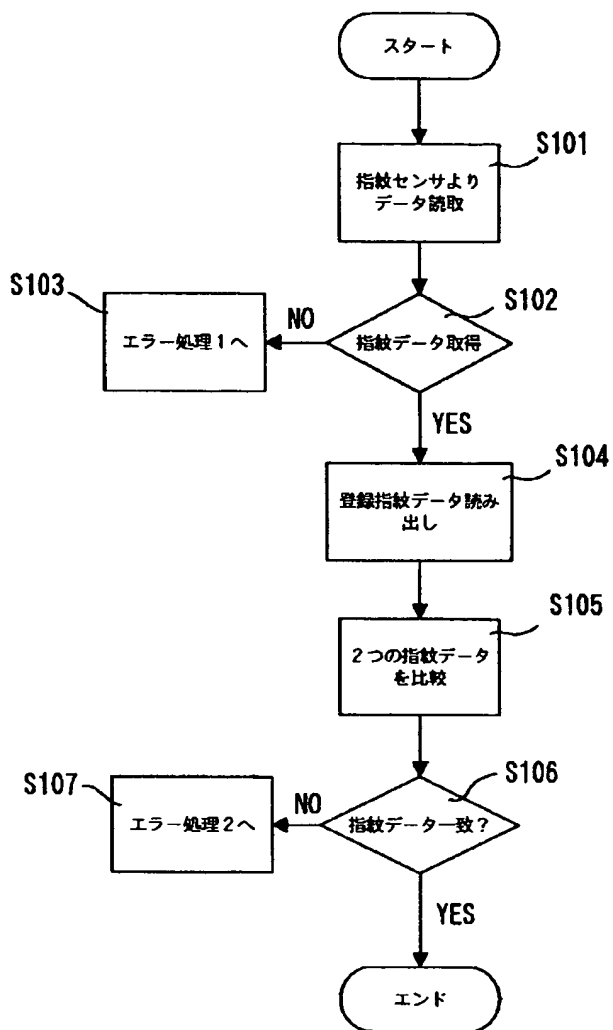
- 1…キーボード
- 2…指紋センサ
- 3…制御部
- 4…認証プログラム保存部
- 5…ユーザ識別データ保存部
- 6…表示部
- 11…電子機器システム
- 12…本体部ケース
- 13…表示部ケース
- 14…ヒンジ部

【図2】



【図3】

【図9】



【図5】

Password =

【図10】

【図12】

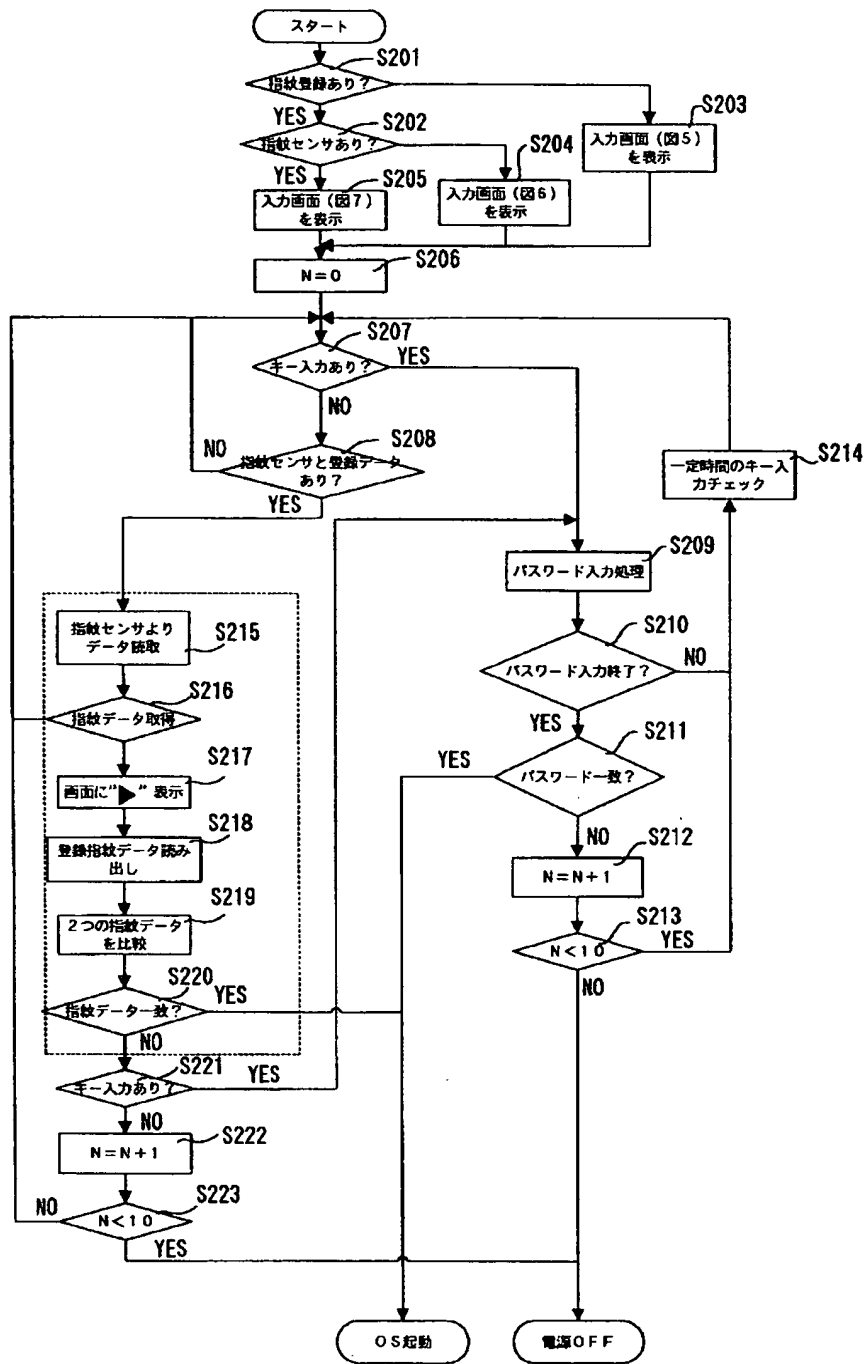
Password =

▶■■■■■|

Password =

|▶▶▶▶▶▶▶▶▶▶|

【図4】



【図 6】

Fingerprint reader not detected.
Password =

【図 7】

Input password or place your finger on the fingerprint reader.
Password =
[Masked input field]

【図 8】

Input password or place your finger on the fingerprint reader.
Password =
Valid password entered, system is now starting up.

【図 11】

Input password or place your finger on the fingerprint reader.
Password =
Verify error.

【図 14】

指紋ユーティリティ

パスワード [Input field]

指紋登録/更新 [Button]

指紋削除 [Button]

キャンセル [Button]

11 (Window title bar)

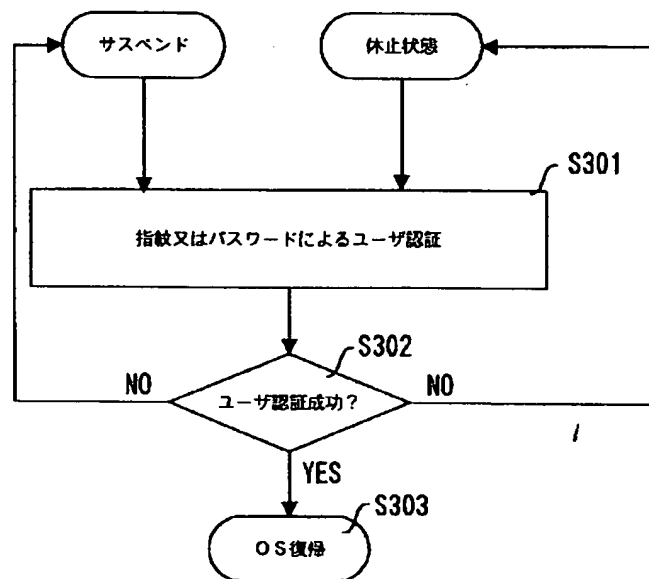
12 (Password input field)

13 (Fingerprint registration/renewal button)

14 (Fingerprint deletion button)

15 (Cancel button)

【図13】



【図15】

